

Use Managed Diversity to Support Endpoint Devices

Ken Dulaney

The rapid influx of privately owned mobile devices demanding access to corporate resources is challenging. Security is being fragmented, leading to policy inconsistencies. To counter, enterprises must implement a structured support system with varied support levels, combined with a push of responsibility and cost out to end users. Enterprises must segment security approaches so that consistency is maintained across all endpoint devices.

Key Findings

- The placement of endpoint platforms under one support group enables an efficient endpoint-support system.
- A homogeneous environment in which everyone has the same device is difficult, if not impossible, to achieve or maintain.
- Many practices that support PCs can be successfully expanded to support other endpoint devices, as long as those policies are expanded to cover the diversity of user demands.
- The implementation of "managed diversity," adapted through the adoption of three levels of support for endpoint devices, will ensure sound device management and cost control.

Recommendations

- Establish a platform support level that permits a narrow set or single choice of hardware when enhanced application support is required. Under our endpoint-device support model, users who need a local-device software image to run enterprise applications that involve local on-device software development are placed under Level 1 platform support.
- Establish an appliance support level for a broader set of hardware choices when applications can be constrained to support solely voice, e-mail, personal information management (PIM) and selected applications that run consistently across the selected hardware.
- Combine the above recommendations with an optional concierge support level that provides hands-on custom support for a fee as an exception. The fee pays for sufficient resources for the individuals whom the company allows to have the flexibility to choose a device.
- Combine platform, appliance and concierge support levels with a number of user groups (generally four to seven groups are recommended) to form a "managed diversity" matrix

that permits more-granular control of security and user expectations for quality of service.

TABLE OF CONTENTS

Analysis	4
1.0 Consign All Endpoint Devices to a Single Support Group	5
2.0 Technology Allocation	5
2.1 The Traditional Approach.....	5
2.2 Managed Diversity and User Choice	6
3.0 Users + Support Levels = Managed Diversity Matrix.....	7
3.1 Understand Endpoint Device Users	7
3.2 Three Levels of Support	7
3.2.1 Level 1: Platform Service.....	7
3.2.2 Level 2: Appliance Service	8
3.2.3 Level 3: Concierge Service.....	10
3.2.4 Key Caveats	11
4.0 What Does Support Include?.....	11
4.1 Data Access and Location, and Its Impact on Security	12
4.1.1 Recommendations	12
4.2 Endpoint Security and Endpoint Data Protection	12
4.2.1 Recommendations	13
4.3 Encryption	13
4.3.1 Recommendations	13
4.4 Authentication/Certificates	13
4.4.1 Recommendations	14
4.5 Endpoint Device Management Software	14
4.5.1 Recommendation.....	14
4.6 Endpoint Application Support.....	14
4.6.1 Recommendations	15
4.7 Backup and Restore	15
4.7.1 Recommendation.....	15
4.8 Attachment Policy.....	15
4.8.1 Recommendations	15
Recommended Reading.....	16

LIST OF FIGURES

Figure 1. Example of a Managed Diversity Matrix	5
---	---

ANALYSIS






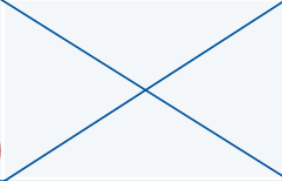



Affordable smartphone models are entering the market in increasing numbers. Organizations face difficulties in selecting a standard device that favors most users. End users routinely disregard IT organization standards (if they exist), choosing instead to adopt whichever device they believe has the features that will satisfy their workplace and personal needs. These features may range from simple conveniences to applications that deliver competitive advantages. As a result, a wide variety of device models is entering the business domain, creating havoc for IT organizations, whose operations are based on standards and stable platforms.


Mobile devices have also fueled consumerization in other areas of endpoint technology, including Windows shops seeing demand for Apple notebooks and departments opting for nonstandard products that they believe more directly affect their business objectives. The increase in technology intelligence that appears in more workers has pushed aside the perception that IT organizations are the experts, and casts them more as technology collaborators. Yet, management still holds IT responsible for many technology functions that IT increasingly cannot control. So, the dilemma is how to ensure that responsibility and authority are conjoined (i.e., where IT is responsible for what it can control and not what it can't control).


Attempts by businesses to ban, discourage and control the use of these devices have been unenforceable. The first offenders are often the executives to whom the IT organization reports. They purchase "the device of the month," then pressure the IT organization to support the new product. BlackBerry and Apple smartphones are examples of devices that IT organizations never wanted inside the corporate domain, but that now demand support.

This research outlines key elements that provide a basis for a support strategy for PDAs and smartphones. This is combined with end-user groups to form a "managed diversity" matrix (a completed example of which is shown in Figure 1).

Figure 1. Example of a Managed Diversity Matrix

Support Level User Groups	Platform	Appliance	Concierge
Executives	E.g., Any Windows phone device 	E.g., Any RIM OS, Windows phone, iPhone OS, Symbian OS or webOS device 	Any device 
Sales Staff	E.g., HP Glisten 	E.g., Any RIM OS, Windows phone, iPhone OS, Symbian OS or webOS device 	
Warehouse Workers	E.g., Motorola MC9500 		

 **IL** Individually-liable (individually owned)

 **CL** Enterprise-liable (aka corporate liable)

Source: Gartner (May 2010)

The remainder of this document is devoted to defining the elements of the above table, as well as providing supporting policies and organizational moves to implement the "managed diversity" concept.

1.0 Consign All Endpoint Devices to a Single Support Group

Organizations will find it hard to achieve an efficient endpoint device support system if all platforms are not placed under one support group. Like PCs, endpoint devices are forms of client access devices, and the policies for them should be similar, if not identical, to those governing PCs. This principle applies not only to smartphones and PDAs, but also to ruggedized handheld devices that are used in specialized applications and desk phones that are increasingly programmable. The practice of managing mobile devices or desk phones in the telecom group, for example, is discouraged, as is the practice of managing ruggedized devices in the business units.

2.0 Technology Allocation

2.1 The Traditional Approach

The general practice for technology allocation is to break up the user community into groups with similar needs, then provide each user in a given group with a portfolio of devices, applications, services and privileges identical to the rest of the group. This is meant to control capital outlays and ongoing support costs. When it comes to endpoint devices, however, this model often fails as the number of endpoint technology options for users explodes. Users find a sense of control through elective technology purchased outside IT mandates. Such personal technology is becoming more available and less expensive, and its users are becoming more adept at circumventing the IT organization's structured environment.

Some Gartner clients report that large user populations, which individually have adopted a technology, will band together to request formal support (for example, for Research In Motion's BlackBerry or the Apple iPhone). Most IT organizations feel forced to procure devices for users to ensure application availability and data security, while controlling device consistency. Eventually, IT budgets balloon as more machines are allocated to individuals under the principle of "sameness" for the user segment. Due to the lack of flexibility of this allocation and support model, individuals often find a means to circumvent policies, leaving the IT department to support personally owned machines (note that ruggedized devices and some other classes may never be individually owned and should be excluded from consideration while reading this document). This endeavor often fails due to a lack of consistency among devices.

2.2 Managed Diversity and User Choice

Standardization helps reduce complexity and total cost of ownership (TCO); however, a completely homogeneous environment is an impossible state to achieve, much less maintain (see "New IT Mandate: Embrace Managed Diversity"). Gartner proposes a managed-diversity approach, which means empowering users with appropriate technology choices and support levels (see "Understanding EA Approaches: Managed Diversity"). Unlike the "one size fits all" approach of most organizations (see "What Is the Right Approach to Developing an Enterprise Architecture?"), managed diversity defines a framework to make additional investments, when appropriate.

Without managed diversity, the organization absorbs costs in three key areas:

- Lost user productivity, because the IT standard does not fit users' needs
- Loss of IT relevance to users, which leads to more self-support and higher indirect costs
- Noncompliance costs incurred by users who work around IT standards

With managed diversity, the IT organization defines what it will do for a given commitment by the end user. Each of these commitments is made depending on what IT can realistically guarantee for service. For example, if IT is permitted to select, own and manage a device, then it can be responsible for the highest quality of service, since it reliably knows the profile against which it will deliver applications. If it is asked to support anything, it is highly unlikely it can provide any such guarantee. In explaining managed diversity to end users, they must be told that, like anything in life, there are privileges and consequences to any decisions they make. And they must understand that each choice will have boundaries, and if those boundaries are crossed, the privileges and consequences will change.

Managed diversity also improves the image of the IT organization in users' minds, because it enables users to make the final decision, rather than forcing the IT organization to select a single solution that may not fit users' work styles. The application of this concept enforces the idea in users' minds that IT is a guide, not a dictator. An increasing number of users who can afford technology and who may have deeper experience levels than IT staff in their organizations often hold the latter image of IT in their minds; managed diversity can dispel this notion.

Managed diversity can be extended to cover costs (not illustrated in Figure 1). Managed diversity improves user satisfaction by permitting users to customize IT funds. Users in each segment are given a predefined list of supported technologies, along with a budget for the projected amount that each selection consumes. Users can optimize the technologies according to their requirements without exceeding the budget. Expense limits and spending caps by individuals bypass the need to rely on subjective interpretations of "reasonable use."

3.0 Users + Support Levels = Managed Diversity Matrix

At its simplest level, the managed diversity framework is a two-by-two matrix that matches user categories or roles to device choices, which are determined by the support level to which the IT organization is willing to commit. Thus, it's crucial to define both users and these support levels, and we recommend that IT organizations select devices in each level.

3.1 Understand Endpoint Device Users

Two prerequisites for implementing an effective endpoint-device support strategy are:

- Understanding users' requirements
- Defining endpoint device workers' profiles based on business impact (see "Provide Appropriate Support Based on Impact Segmentation") and on how they work

Consider the value that endpoint-device technology and relative support have for the user and for the business. Furthermore, an endpoint-device user base can be segmented according to where users work (that is, the location, amount of work-related travel and distance traveled, and work style). Consider the applications they use, as well as the type of connectivity and the amount of bandwidth they require. To manage segmentation, limit the number of profiles. In most cases, four to five suffice. (For a wider discussion of users' segmentation, see "Overviewing the Three Vectors of Mobile Worker Segmentation.")

3.2 Three Levels of Support

We suggest a model that includes three levels of support for endpoint devices. These levels are exhaustive. No device should sit outside the levels; all are taken into account. Furthermore, as new devices are added to a level for support (models change frequently), other devices are eliminated from the support model. This keeps the list of supported devices in each level from growing exponentially and facilitates an end-of-support policy.

3.2.1 Level 1: Platform Service

Level 1 provides full support, similar to that for PCs and notebooks in most organizations. To provide this level of support, the IT organization must select a platform and a device, or set of devices, for the PDA and smartphone categories. This implies that there will be a "business standard PDA" and a "business standard smartphone." For mobile devices, only smartphones are in this class, because standard cellular phones are not IT-level programmable devices and are used only as thin-client voice terminals. Such devices have few tools to integrate with the IT environment and pose few threats. If users select this "business standard" hardware, then the IT organization will purchase the unit for them, track it during its lifetime, provide for breaks and fixes, develop applications for it and answer questions about its use — the same privileges that are granted for standard PCs and notebooks.

The value proposition for users in this scenario is that, if the user keeps the hardware choice constrained, then IT will provide application flexibility. This means that IT will bring to bear its resources to develop, deploy and maintain any application that the business demands, funds and that can realistically be supported. IT can provide only a broad set of applications when the devices targeted for these applications are relatively few and offer strong security and management tools. Developing applications for any device, even when employing tools such as Mobile Enterprise Application Platforms (MEAPs), raises costs. End users who find themselves initially at one of the other support levels should understand at the outset that changing their requirements to include application support necessitates a change in privileges and consequences, because they are changing support levels. In essence, the platform service level

is the traditional approach of enforced standardization through controlled ownership. However, because the platform is part of the managed-diversity framework, accountability doesn't end here. Out-of-bounds conditions will be accounted for fully, as described in the following sections.

Platform levels should follow established IT policies for notebooks and desktops. Failure to do so makes the platform policy hypocritical. For example, many organizations commit to Windows-based hardware products, because a variety of suppliers are ensuring that the purchases can be price-competitive and that backup hardware vendors are available, should an incumbent vendor fall into disfavor or experience supply interruptions. If IT places a product that is solely sourced at the platform level, it should recognize that it is compromising its own well-established policy and has introduced risk. If an application is built for a sole-source device and that device is unavailable because of vendor failure, for example, then there is no recourse, and the quality-of-service commitment made by IT for this user commitment cannot be met.

So, in the end, when users select their platform level, they constrain their hardware choices in return for a guarantee by IT for a given level of quality of service. Although this has always been the offer in the past, IT forced this choice upon its users. Now, users are asking for a commitment, in return, for the particular service they expect.

3.2.2 Level 2: Appliance Service

This is the "linchpin" of the managed-diversity strategy, providing support for personally owned endpoint devices (individually liable), as well as business-appliance-style devices (enterprise-liable, aka corporate-liable). Appliance service ensures business information integrity by constraining the supported applications. Level 2 provides support for voice, basic browsing, PIM and e-mail (and, possibly, other cross-device applications provided by a particular software application vendor), as long as the user interfaces through software that is selected by the business. This narrowing of the permitted functionality is the reason for the term "appliance" in the description of this level.

There are some deviations from the above premise. Offline applications that are supported across multiple platforms can also fall into this category (for example, if salesforce.com is built to support several devices, those can be considered appliances). But enterprises should be forewarned that, if other applications are added, any one that violates the policy forces it to move the platform level. Also, browser applications can be considered part of the appliance level, since there is no code resident on the device. And, in the future, as HTML 5 begins to incorporate offline capabilities through standards, those may also be included, since they are operating-system-neutral.

In essence, the appliance service level reverses the value proposition stated in Level 1. In Level 2, device choice is permitted in return for application constraint, whereas the platform level enables application choice in return for hardware constraint. Other applications may be on the device, but they will not be supported; users will be directed to the application provider or mobile operator for support (e.g., for games or other personal applications). Many support organizations claim that they get calls on out-of-band applications, regardless of the device choice, but the IT organization must ensure that it creates and adheres to a policy that rejects these inquiries; otherwise, the entire plan will fail. The appliance level reduces organizational stress by permitting the user to take advantage of more device options, as long as the organization reduces what the device can do. Most organizations that have enforced this level only take questions on failures of e-mail and PIM delivery, rejecting all other queries.

Gartner requires that an appliance device support at least two security policies. The first permits the device to be cleaned of all content "over the air" (OTA), should the device be reported as lost or stolen. The second forces the user to employ a complex password consisting of a combination

of uppercase and lowercase letters, numbers and special characters, with the ability for periodic changes.

Encryption is now a suggested option for appliance-level devices. If a device meets the above baseline security requirements and has an encryption capability, it should be invoked as an extra measure of protection. This is suggested even when it causes some user inconvenience, slight performance degradation or has not been proven in all tested security scenarios. Encryption will remain a suggested option until YE11, at which time, we believe, most mainstream endpoint operating systems with at least 10% share of their respective market will have robust solutions. At that time, we expect to make encryption mandatory. Gartner will continue to assess endpoint encryption, and will publish its findings in current and future research.

In the appliance level, the devices may be either individually or enterprise-labile. As more and more organizations find that they do not have the resources to support devices that have rapid turnover, they are pushing devices toward individually liable plans (a counterpoint to this direction is discussed in "Companies Should Keep Control of Cellular Users Through Corporate Liability"). This is possible because typical business e-mail applications have built-in defense mechanisms that permit user devices to connect onto the enterprise network, while protecting propagation of spam and other malicious software across the enterprise. All other applications typically require protection from a perimeter defense mechanism, which, if breached, can provide access to many sensitive applications.

Organizations that permit individually liable devices to connect to enterprise e-mail systems under the appliance level must require the user to sign documents that enforce at least three policies:

1. As a condition of employment, the end user must report any lost or stolen device to IT immediately upon detection.
2. When reported lost or stolen, the user grants permission for the device to be wiped of its contents. This policy is necessary to ensure that an end user who has invested in personal music, but who hasn't backed it up, doesn't make a compensatory claim for reimbursement.
3. And, lastly, to prevent misuse, users must be told that these devices are for their own convenience, but that all e-mail and attachments must be read on standard PCs and notebooks. This prevents the user from believing that a mobile or other non-PC endpoint device is a notebook substitute and blaming IT for any document conversion mistakes inherent in non-Windows platforms.

One additional function sometimes required for the connection of individually liable devices to the enterprise systems is the requirement of a certificate to prevent the end user from giving access credentials to other users. This is potentially a complex initiative and is discussed in other research on public-key infrastructure (PKI) techniques. For a brief discussion of certificate use and other alternatives, see Note 1. Encryption is another optional item to protect the data (see "Highlights From the Security and Risk Management Track at Symposium/ITxpo" and "Magic Quadrant for Endpoint Protection Platforms").

The appliance level helps give users what they have been looking for: the ability to choose from popular devices (within reason). The option for the user to select from a list of devices implies that the IT organization will, at a minimum, select PIM and e-mail back-office synchronization applications that support a wide range of consumer handhelds. By forcing users to employ the business standard for synchronization, instead of the application that came with the device, businesses can enforce policies and gain control of data movement. At this level of support, businesses should, at a minimum, choose e-mail, PIM and other applications that secure themselves, and that require access control methods from the server. Security software that

enforces power-on passwords and encryption of stored data should be installed, as it is for notebook PCs. Security requirements may vary from one organization to another (see "Magic Quadrant for Enterprise Wireless E-Mail Software Market").

There are additional issues regarding both individually and enterprise-liable devices. If the enterprise decides to purchase the device, then the enterprise may provide better service to individuals or may be part of a larger contractual agreement. However, Apple iPhones and BlackBerry devices often are placed at the appliance level, because their unlicensed software platforms do not provide for backup hardware vendors. This can make it difficult to put these vendors in the platform category, where offline code is developed. Even so, BlackBerry and Apple can provide browser-based applications that keep them in the appliance category, since no local code has been developed. The development of local code is what moves a device to the platform level. Android, at the time of this writing, did not support the password policy and could not be put into the appliance or the platform level of support. Gartner continually tests the various popular devices it receives for compliance at the appliance level and will update its positions over time.

By accommodating a variety of personally owned devices, the IT organization creates a safety valve for the inevitable claim from users that there is something better on the market. This also enables users to capture individually driven productivity requirements.

Increasingly, IT organizations report a strong move to individually liable mobile devices (others are kept enterprise-liable because they reside in the enterprise or change infrequently). These organizations require the user to purchase the device from his or her own funds, or provide a biannual stipend (to coincide with the typical two-year, mobile-services contract and the typical life span of a mobile device). The trend is driven by the ability to save money by capping the amount that the organization is willing to spend (iPhone buyers must supplement the stipend with their own funds, if necessary) and the ability to push some support back to the mobile operator. When the device breaks, it's the user's responsibility to contact the carrier for repair.

3.2.3 Level 3: Concierge Service

Occasionally, users demand support from the IT organization for any device they acquire. These users often are found in the executive group. The pressure to support them is high because IT often must report to these individuals. In rare exceptions, the IT organization can accommodate such requests by charging a monthly fee that is high enough to discourage casual inquiries, but sufficient to pay for the custom service required for a device that may not have even minimum security (see "Four TCO Profiles for Smartphones and PDAs: 2009 Update"). For this fee, IT supplies on-call resources that perform whatever functions are necessary to support the executives. Each incident requires IT to address the security of data applications, and likely will require a high degree of manual intervention. The resources (internal or external) that are needed to perform such tasks are funded entirely by the fee paid by such users. The establishment of a concierge service level as a bill-back system should be viewed as a means to encourage nonconformist users to adhere to established policies.

Placing a device on the concierge level solicits one of two reactions:

- Agreement to pay the fee
- Refusal to pay the fee, accompanied by a threat that IT must support the device or lose support from management

In the latter case, we suggest that the IT organization create a budget line item called "concierge service" and charge an appropriate amount into this account each month so that, at the end of the year, the work done to support such devices is positively accounted for. This enables the IT organization to establish an important cultural connection between "exceptions" and "costs" that

may be challenging to create, but will prove valuable in the long term, if the concept of managed diversity is extended to other areas.

3.2.4 Key Caveats

- One of the core principles of managed diversity is to enable IT to say yes to whatever the user wants, but force the user to see the impact of his or her decisions. This must be clearly evident in any documentation in the program distributed to end users.
- Account for everything. There has always been a tendency for IT support staff to deal with exceptions for free. Especially for concierge devices, the amount of time spent on such extra activities can pile up, causing other important activities to be neglected.
- Don't ignore exceptions that may lead to security breaches. Doing so creates a perception among users that IT is an organization that always can find a way to support their needs. This exception mentality must be changed to a viewpoint where the user recognizes that he or she must pay for services, and that there are trade-offs with any request. Also, ignored security issues permit a persistent scenario where routes around IT policies are the norm, creating a worse problem if IT is ever audited.
- Establish channels for users to bring forward ideas regarding new technologies, applications and support options.
- Don't accept consequences that are the responsibility of the user. Often, IT organizations seek to gain favor by thinking through the requirements and making decisions on behalf of the users. However, end users increasingly want to make their own decisions. In such cases, they also must accept the consequences. IT must avoid shouldering the outcome of these decisions on users' behalf.
- Unstructured support (that is, treating everything as an exception) risks transforming every user into a "concierge" user, from a TCO perspective. In this case, the cost of support can be more than 90% higher, because there is no economies of scale, but lots of manual management.
- If the device is employee-owned, and if you don't support it at all, then you could incur extensive security and privacy risks, which are not easily quantifiable.
- This framework cannot guarantee the lowest possible TCO, but it does ensure choice and some degree of control.

4.0 What Does Support Include?

Support ensures that users can work with their devices, minimizing downtime and lost productivity, while guaranteeing data and application security. Depth of support is determined by the level of privileges that is granted to each user. IT should set clear expectations by defining competencies and responsibilities, and by establishing policies and processes. In the case of the Level 1 platform, IT will manage endpoint devices throughout all the various stages of the life of the device, from hardware and service plan procurement to disposal and service termination. For individually liable and enterprise-labile devices under Level 2 appliance support, IT's responsibility for support is limited to operational support applications that are used and their related security requirements. This enables organizations to control data flow and its security. Level 3 concierge support is customized and delivered to whatever level the user is willing to pay. The service level and the amount to be charged for that service must be negotiated with the user constituency.

The next section discusses, in more detail, some elements of support.

4.1 Data Access and Location, and Its Impact on Security

Synchronization is the method by which e-mail, PIM and other data on an endpoint device are downloaded to an application (for example, e-mail and PIM to Microsoft Outlook), saved and updated to reflect the changes that have occurred since the last synchronization. Typically, the information also includes contacts, task lists, appointments and notes.

Many endpoint devices — especially the mobile ones — come with powerful, easy-to-use tools that enable rapid interface to business systems. When end users install such tools, they "punch a hole" through the enterprise security perimeter, permitting data to be moved across applications to personally owned devices without the IT organization's knowledge or control. Many organizations that believe this is under control find, during any audit, that they have an increasing amount of information on uncontrolled or external content stores.

Although the front end of most organizations is protected by firewalls and other security technologies, many of the devices used to interact with enterprise systems can also be used as conduits of information to foreign devices. Thus, the security framework is protected only by the good intentions of the employees. User training often is inadequate, and employee responsibilities are poorly defined. Once an organization's data resides on personal machines, the business can do little to protect and secure the information. It is, therefore, important to view managed diversity as a means to move hidden activities to the visible forefront of activities through appropriate segmentation, which, in turn, permits some of the flexibility the user seeks within the reasonable limits of risks posed by that particular group.

4.1.1 Recommendations

- Synchronize the content on devices to the enterprise core. This will disallow two-step synchronization to the PC and then to the endpoint device (see "Magic Quadrant for Enterprise Wireless E-Mail Software Market"). Synchronization to the PC and to the device may leave open ports that can be further exploited, as well as create the potential for data to be out of synch, causing errors.
- Address the costs that are associated with synchronization to the core by securing cellular pricing plans that discourage synchronization through the PC. Also, devices without cellular service can be forced into synchronization through the locally attached PC (versus the two-step process) and directly to the core.
- Select a business standard for synchronization and e-mail gateway software when implementing the three levels of support for endpoint devices. This software must reside at all points of entry for such devices — at the server for wireless devices that synchronize against applications, such as e-mail, and at the desktop for devices that connect via cable or other personal-networking means.
- Maintain an aggressive stance toward supporting more devices as they become popular and meet the minimum security requirements under the appliance level.

4.2 Endpoint Security and Endpoint Data Protection

Endpoint device security and data protection systems and procedures protect user privacy and enterprise data, and they help enterprises comply with audit requirements. Endpoint device security products include Secure Sockets Layer virtual private-network solutions and firewalls. Data protection products for endpoint devices primarily offer encryption, but are expanding to include user authentication, policy management and value-added features, such as the protection

of information on removable media. Other functionalities include centrally managed access controls, lockouts and recovery methods (see "Magic Quadrant for Mobile Data Protection"). Every company must include these functionalities in its IT operations plan.

4.2.1 Recommendations

- Ensure that the policies regarding security and endpoint data are consistent across different matrix entries of the managed diversity framework.
- Procure devices for employees, if the highest level of security is needed. The use of individually liable devices is acceptable only when critical applications and sensitive data are not required, or when applications can be constrained to what is described under the appliance level.

4.3 Encryption

Data exposure is an important issue, exacerbated by the expansion of onboard device storage capabilities, increasing the amount of data at risk for theft, loss or misuse.

4.3.1 Recommendations

- Define clear and strict guidelines on the amount and type of business information that can be stored on endpoint devices, and on what data can be accessed and transferred through these devices. Include guidelines about which items can be moved out of the secure corporate environment and which data should be encrypted. Although data that is likely to move requires encryption, not all corporate data needs it, and software encryption and decryption may degrade the performance of older devices.
- Implement data encryption for all data that is stored on endpoint devices. Secure the data on peripheral storage devices.
- Encourage the use of built-in security features for data protection, such as those integrated by endpoint operating-system providers. Endpoint data security tools offer various degrees of encryption strengths at different levels (for example, files, folders, partitions and full disks).
- Ensure that encryption is a policy enforced through back-office applications. Do not permit end users to decide whether encryption is deployed.

4.4 Authentication/Certificates

Many organizations still rely on passwords for user authentication. Passwords are the most commonly used security practice, but these rarely are managed effectively. Password-enforcement tools can be installed at the back end to ensure that passwords go through routine audits that set expiration dates and enforce the use of "strong" passwords. Certificates permit IT to provide more-granular control over which devices are requesting enterprise access. Organizations offering appliance-level support may wish to ensure that access credentials cannot be easily transferred to other endpoint devices without permission.

Note 1 discusses methods to ensure that only authorized devices are connecting to the enterprise network.

4.4.1 Recommendations

- Do not allow full access to corporate resources when remote-user and device authentication is weak. Rather, authorize access depending on the level of trust in the user and in the device.
- Couple the use of passwords with more-advanced authentication methods. Strong authentication products that use icons, tokens and biometrics are available, but these often lack user friendliness. In addition, a server-side wiping function can be implemented to remove all data remotely, if the device is lost or stolen.
- Consider the use of third-party certificate management products if not available natively through an operating system platform.

4.5 Endpoint Device Management Software

Endpoint device management software automates tasks such as inventory, asset management, hardware configuration, software distribution, monitoring data and application use, and application management. We recommend processes similar to those that are used for PCs and notebooks; however, no single suite supports all the functionalities and endpoint computing devices that support these processes.

Traditional PC configuration management vendors have been slow to address the needs of smaller devices. Endpoint device management software suites focus on endpoint devices and notebooks only, and have little integration with the PC configuration management tools that organizations are likely to have in place. There is a path to convergence between these tools, but it is some time away. Mobile e-mail management suites increasingly include management and security features. The mobile operator, in many cases, provides OTA management services, but these services often run parallel to IT-supplied management tools.

IT organizations should be careful when layering in management tools on top of other applications that may independently synchronize information. Synchronization is a battery-consuming technique, and parallel activities can shorten battery life.

4.5.1 Recommendation

- Work with mobile-operator vendors to ensure that updates don't interfere with the operation of mission-critical software on the device. (For further details, see "The Five Phases of the Mobile Device Management Life Cycle.")

4.6 Endpoint Application Support

Under our model, devices that run enterprise applications involving local, on-device software development are placed under Level 1 — platform support. The idea is to limit the number of hardware platforms that optimize the skills that are required to develop and support such customized code. Application developers who cannot target a stable, narrow hardware platform will see a tremendous increase in difficulties in delivering application quality of service.

This doesn't imply that, under Level 2, only voice, PIM, e-mail and browsing should be supported. Applications can be delivered under Level 2, but it is a best practice to select applications that run across a number of different platforms so that, if difficulties with one hardware vendor arise, then it is possible to move to another with minimal user retraining. Generally, these are third-party applications where the supplier continually delivers and tests its application on multiple hardware offerings and operating systems. Internal-development efforts can follow this path, but often don't because of the costs. If an internal effort targets a single device/operating system, then it requires a Level 1 device. Web-based applications that are accessible through the browser are a good

way to distribute applications while retaining devices under Level 2 support. Browser applications can also provide cross-operating-system support, although they may not work offline when out of coverage.

Gartner research on MEAPs (see "Magic Quadrant for Mobile Enterprise Application Platforms") discusses software development products that permit a single development effort to dynamically deliver output (or receive input) to a variety of endpoint devices (despite the mobile name). This software can be used to maintain support for Level 1 or Level 2 devices. It involves using a single model for back-end data access and logic with a device-driven mechanism that dynamically transforms output to the resource profile of the requesting device. There is maintenance to maintain the screen transformations, but it is far less than separate applications.

4.6.1 Recommendations

- Keep applications other than e-mail and PIM running on Level 1 devices, as a general rule.
- Organizations should keep their MEAP products under Level 1 devices to ease the pain of supporting more than one dedicated device. MEAPs can also ease maintenance under Level 2 support, but may not reduce risk when used on individually liable devices.

4.7 Backup and Restore

The information on some endpoint devices can be erased when the batteries run out of power, the device is damaged or as a security measure. Given the highly mobile and battery-dependent nature of mobile devices, one of these occurrences is certain to happen to one user or another. Centralized backup and restore capabilities enable the recovery of information on lost, damaged or dead devices.

4.7.1 Recommendation

- Move stored data and recovery information from the user's desktop to a back-end system. This enables better administrative control and subjects the data to corporate backup policies, rather than leaving it in the hands of the user.

4.8 Attachment Policy

As mentioned earlier, users often request the capability to read attachments on endpoint devices. Attachment readers can take most Microsoft Office files and render their images on the small screen, which is a valuable feature when an attachment is key to understanding an e-mail. However, attachment readers produce a format similar to that of PDFs. They are unable to deal with embedded features, such as macros and formulas. There is no way to tell where compatibility with Microsoft Office ends and incompatibility begins. This means that a spreadsheet with embedded macros is unlikely to guarantee operational compliance with its PC-based cousin — basic Microsoft Office. This situation is not expected to change in the near term, because reaching this goal involves the complete porting of Microsoft Office over to another platform.

4.8.1 Recommendations

- Get the message across to users that, regardless of the level of support granted, compatibility cannot be guaranteed; the IT organization will not be responsible for problems that might occur.
- Users should be required to read all e-mail on standard PCs or notebooks using the official business software image.

RECOMMENDED READING

"Implementation Advice for Mobile Data Protection"

"How to Avoid Mobile Data Protection Failures"

"How to Develop an End-to-End Policy for Enterprise Mobility"

"New IT Mandate: Embrace Managed Diversity"

"Gartner's View on Enterprise Mobility"

"Magic Quadrant for Endpoint Protection Platforms"

Note 1

Controlling Device Access

Here, we provide references that discuss how to prevent unauthorized devices from connecting to native e-mail systems (third-party products typically have this feature integrated with their offerings).

Since Microsoft Exchange is the largest installed based, we offer the following three based on a working environment of Exchange and Microsoft Intelligent Application Gateway (IAG), using ActiveSync for synchronizing mobile devices. For users of other e-mail systems, we suggest a conversation with your providing vendor, using this document as a guide for finding similar solutions within that environment.

Filter for iPhones at the Firewall

There are several references on the Internet that show how to filter iPhones (for example, as a device class). The references say that the HTTP header on packets from the iPhone can be blocked by a signature. The following hyperlink provides step-by-step instructions for the ISA firewall, but should work on other firewalls too (see <http://wmpoweruser.com/?p=1023>). It appears that IAG contains the ISA firewall, so the configuration should be the same.

For advanced firewall filtering, see <http://msexchangeteam.com/archive/2008/09/05/449757.aspx>, which provides an illustrated tutorial about three ways to block devices, and finishes with details on setting firewall filters. The best solution is to combine firewall signature filters with a business process to only enable user access by device ID and device type when a smartphone is provisioned.

Filter for Device ID Within Exchange Server

<http://brendanz.net/?p=6> shows how to filter for devices based on device ID. Using this method, IT can limit the number of device IDs that are bound to a user ID. In practice, the tech support group would need to enroll the correct user device and bind only the desired device ID. You can also use the report generated to compile a list of all devices that your users are currently using.

The command that generates the report is Get-ActiveSyncDeviceStatistics, and it's explained at <http://technet.microsoft.com/en-us/library/aa996908.aspx>.

The attribute that enables allowed device ID is ActiveSyncAllowedDeviceIDs, and it's explained at <http://technet.microsoft.com/en-us/library/bb125264.aspx>.

The following are specific instructions from a client who has implemented this technique:

A script can be run on the Exchange server: `Get-Mailbox-ResultSize:unlimited-server ACTUAL SERVER NAME HERE | ForEach {Get-ActiveSyncDeviceStatistics-Mailbox:$_.Identity} | Where {$_ .LastSuccessSync-gt '2/15/2009'} | Select-Object @{name="EmailAddress";expression={$_ .Identity.ToString().Split("\")[0]}},DeviceType,DeviceModel,DeviceID,LastSuccessSync | Export-Csv-Path:"C:\temp\MobileDevices_ACTUAL SERVER NAME HERE.csv"`

Based on the result of the script, the tool provides a spreadsheet that can be sorted by device type. If someone is connecting with an unsupported device, the account can be disabled. Of course, this would not be suggested in high volume of abuse situations or where immediate corrective action is necessary.

Also see [http://technet.microsoft.com/en-us/library/aa997489\(EXCHG.65\).aspx](http://technet.microsoft.com/en-us/library/aa997489(EXCHG.65).aspx).

Employ Device Certificates

The alternate (or in addition to) way of authenticating a device is to use certificates, assuming that the deployment entity is comfortable with the process for certificate management. Here is a more detailed description of one way to implement certificates for Microsoft Exchange management: Microsoft provides an Exchange Server ActiveSync Certificate-Based authentication tool with several utilities to assist in configuring and validating client certificate authentication. Mobile devices are supported. The tool is described at this address:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=82510E18-7965-4883-A8C3-F73F1F4733AC&displaylang=en>.

A simpler alternative may suffice if the IT organization feels formal certificates are not warranted. The device ID associated with a phone is supposed to be unique, and if changeable, is beyond the means of users. The device ID is described at

http://publib.boulder.ibm.com/infocenter/wedmlInfo/v6r0/index.jsp?topic=/com.ibm.websphere.dms.doc/dm/sphone_tasks_device_id.html.

This research is part of a set of related research pieces. See "ATV: Guide for Mobile Application Development, Sourcing and Support" for an overview.

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509